

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (currently amended): A system for providing secure exchange of
2 sensitive information with an implantable medical device, comprising:
3 a crypto key uniquely associated with an implantable medical device to
4 encrypt sensitive information during a data exchange session; and
5 an external source, comprising:
6 a key module configured to securely obtain the crypto key over a
7 secure connection from a secure key repository securely maintaining the crypto
8 [[key,]] key and further configured to encrypt the sensitive information using the
9 crypto [[key,]] key;
10 a long range transmission module configured to transmit the
11 encrypted sensitive information to the implantable medical device via a long
12 range interface and further configured to store the encrypted sensitive information
13 as encrypted data onto the implantable medical [[device,]] device; and
14 a short range transmission module configured to further [[store]]
15 transmit a copy of at least a part of the sensitive information to the implantable
16 medical device via a secure short range interface and further configured to store
17 the copy as unencrypted data onto the implantable medical device ~~over a secure~~
18 ~~connection.~~
- 1 2. (currently amended): A system according to Claim 1, ~~further~~
2 ~~comprising a~~ wherein the short range interface [[to]] logically ~~define~~ defines a
3 secured area around the implantable medical device within which to securely
4 obtain the crypto ~~key;~~ and a and the long range interface [[to]] logically ~~define~~
5 defines a non-secured area extending beyond the secured area within which to
6 exchange the encrypted data.

1 3. (original): A system according to Claim 1, wherein the encrypted
2 data is retrieved from the implantable medical device over a non-secure
3 connection and the encrypted data is decrypted as the sensitive data using the
4 crypto key.

1 4. (original): A system according to Claim 3, wherein the crypto key
2 is securely retrieved over a secure connection from the secure key repository prior
3 to decrypting the encrypted data.

1 5. (original): A system according to Claim 3, wherein the encrypted
2 data is retrieved through long range telemetry.

1 6. (original): A system according to Claim 5, wherein the long range
2 telemetry comprises radio frequency telemetry.

1 Claim 7 (canceled).

1 8. (previously presented): A system according to Claim 1, wherein
2 the unencrypted data is securely retrieved from the implantable medical device
3 over a secure connection.

1 9. (original): A system according to Claim 1, wherein the crypto key
2 is securely retrieved from the secure key repository through a programmer.

1 10. (original): A system according to Claim 1, wherein the crypto key
2 is maintained on the implantable medical device, and the crypto key is retrieved
3 through short range telemetry.

1 11. (original): A system according to Claim 10, wherein the short
2 range telemetry comprises inductive telemetry.

1 12. (original): A system according to Claim 1, wherein the external
2 source comprises at least one of a programmer and a repeater.

1 13. (original): A system according to Claim 1, wherein the crypto key
2 comprises an encryption key in accordance with the Advanced Encryption
3 Standard.

1 14. (currently amended): A method for providing secure exchange of
2 sensitive information with an implantable medical device, comprising:
3 defining a crypto key uniquely associated with an implantable medical
4 device to encrypt sensitive information during a data exchange session;
5 securely obtaining the crypto key over a secure connection from a secure
6 key repository securely maintaining the crypto key;
7 encrypting the sensitive information using the crypto key, transmitting the
8 encrypted sensitive information to the implantable medical device via a long
9 range interface, and storing the encrypted sensitive information ~~as encrypted data~~
10 onto the implantable medical device; and
11 ~~storing~~ transmitting a copy of at least a part of the sensitive
12 information to the implantable medical device via a secure short range interface
13 and storing the copy as unencrypted data onto the implantable medical device
14 ~~over a secure connection.~~

1 15. (original): A method according to Claim 14, further comprising:
2 logically defining a secured area around the implantable medical device
3 within which to securely obtain the crypto key; and
4 logically defining a non-secured area extending beyond the secured area
5 within which to exchange the encrypted data.

1 16. (original): A method according to Claim 14, further comprising:
2 retrieving the encrypted data from the implantable medical device over a
3 non-secure connection; and
4 decrypting the encrypted data as the sensitive data using the crypto key.

1 17. (original): A method according to Claim 16, further comprising:

2 securely retrieving the crypto key over a secure connection from the
3 secure key repository prior to decrypting the encrypted data.

1 18. (original): A method according to Claim 16, further comprising:
2 retrieving the encrypted data through long range telemetry.

1 19. (original): A method according to Claim 18, wherein the long
2 range telemetry comprises radio frequency telemetry.

1 Claim 20 (canceled).

1 21. (currently amended): A method according to ~~Claim 21~~ Claim 14,
2 further comprising:
3 securely retrieving the unencrypted data from the implantable medical
4 device over a secure connection.

1 22. (original): A method according to Claim 14, wherein the crypto
2 key is securely retrieved from the secure key repository through a programmer.

1 23. (original): A method according to Claim 14, further comprising:
2 maintaining the crypto key on the implantable medical device; and
3 retrieving the crypto key through short range telemetry.

1 24. (original): A method according to Claim 23, wherein the short
2 range telemetry comprises inductive telemetry.

1 25. (original): A method according to Claim 14, wherein the external
2 source comprises at least one of a programmer and a repeater.

1 26. (original): A method according to Claim 14, wherein the crypto
2 key comprises an encryption key in accordance with the Advanced Encryption
3 Standard.

1 27. (currently amended): An apparatus for securely transacting a data
2 exchange session with an implantable medical device, comprising:
3 means for defining a crypto key uniquely associated with an implantable
4 medical device to encrypt sensitive information during a data exchange session;
5 means for securely obtaining the crypto key over a secure connection from
6 a secure key repository securely maintaining the crypto key;
7 means for encrypting the sensitive information using the crypto key,
8 means for transmitting the encrypted sensitive information to the implantable
9 medical device via a long range interface, and means for storing the encrypted
10 sensitive information as ~~encrypted data~~ onto the implantable medical device; and
11 means for further ~~storing~~ transmitting a copy of at least a part of the
12 sensitive information to the implantable medical device via a secure short range
13 interface and means for storing the copy as unencrypted data onto the implantable
14 medical device over a secure connection.

1 28. (currently amended): An implantable medical device for securely
2 maintaining sensitive information, comprising:
3 an implantable medical device, comprising:
4 a receiver to receive sensitive information via a long range
5 interface and a copy of at least a part of the sensitive information via a short range
6 interface;
7 a memory to store the sensitive information encrypted using a
8 crypto key uniquely associated with an implantable medical device and ~~at least a~~
9 ~~part of the sensitive information~~ the copy as unencrypted data; and
10 a secure interface to provide access to the stored sensitive
11 information exclusively over a secure connection.

1 29. (currently amended): An method for securely maintaining sensitive
2 information on an implantable medical device, comprising:

3 receiving sensitive information via a long range interface and a copy of at
4 least a part of the sensitive information via a short range interface;
5 storing the sensitive information encrypted using a crypto key uniquely
6 associated with an implantable medical device and ~~at least a part of the sensitive~~
7 ~~information~~ the copy as unencrypted data; and
8 providing access to the stored sensitive information exclusively over a
9 secure connection.

1 30. (currently amended): An apparatus for securely maintaining
2 sensitive information on an implantable medical device, comprising:
3 means for receiving sensitive information via a long range interface and a
4 copy of at least a part of the sensitive information via a short range interface;
5 means for storing the sensitive information encrypted using a crypto key
6 uniquely associated with an implantable medical device and ~~at least a part of the~~
7 ~~sensitive information~~ the copy as unencrypted data; and
8 means for providing access to the stored sensitive information exclusively
9 over a secure connection.